DATA SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING

***Nirmala.S**
Assistant Professor
Sambhram Academy of Management Studies, Bangalore.

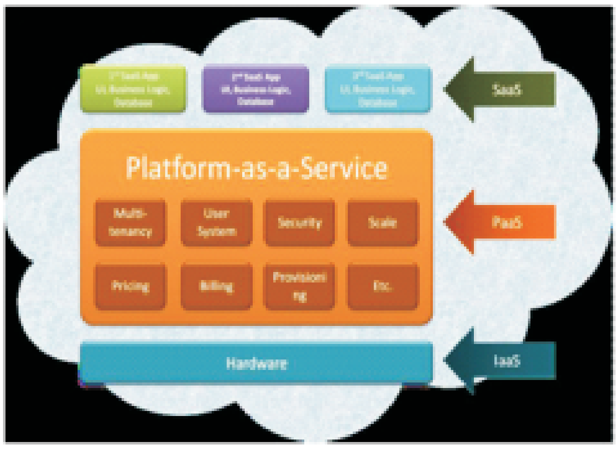
ABSTRACT

Cloud Computing refers to applications & services that run on a distributed network using virtualized resources & accessed by common internet protocols and networking standards. Services are offered to the users over the web on pay-per-use on demand. Cloud services are provided by a third party supplier who possesses the arrangement. Cloud Computing has many advantages such as flexibility, efficiency, scalability, integration and capital reduction. In spite of possible benefits security is one big challenge that is hindering the growth of cloud computing. Various security challenges and issues are there for all the Service Delivery Models. Infrastructure as a service (IaaS) is a foundation layer to all the other Service Delivery models. Lack of security in this layer will certainly affect the other Service Delivery Models i,e PaaS & SaaS, which are built upon IaaS Layer. In this paper we present an elaborated study of Data Security which is a part of IaaS components security and determine vulnerabilities & countermeasures.

1. INTRODUCTION

Clouds are large pools of easily usable & accessible virtualized resources. These resources can be dynamically reconfigured. Cloud computing incorporates virtualization, on-demand deployment. Cloud computing is a technology that uses the internet and central remote servers to maintain data & applications. Cloud Service providers mainly offer three service delivery models that are SaaS, PaaS & IaaS.

IaaS layer provides the primary infrastructure of the cloud as a service to the customers. Infrastructure is the main H/w components &their management S/w that includes Services, Network, Storage, File systems, Operating System.


1st SaaS App UI, Business Logic, Database
2nd SaaS App UI, Business Logic, Database
3rd SaaS App UI, Business Logic, Database
SaaS
Platform-as-a-Service
Multi-tenancy
User System
Security
Scale
Pricing
Billing
Provisioning
Etc.
PaaS
Hardware
IaaS

Securing IaaS layer is divided into two main areas, the virtual environment and the Physical environment. Several security requirements need to be present at the virtual level which includes controlling access, Data Encryption, Secure communication channels & virtual protection. On the other hand in the physical environment it is required to ensure H/w reliability & preventing physical intrusion.

To achieve Data Security there is a critical need to securely store, manage, share &analyze the massive amounts of complex i,e semi-structured & unstructured data.

The nature of the application requires the clouds to be secure. The major security challenge with clouds is that the owner of the data may not have control over where the data is placed. Therefore we need to safeguard the data in the midst of the un trusted processes.

The emerging cloud computing model attempts to address the explosive growth of web-connected devices and handle massive amounts of data. Google has now introduced Map-Reduce framework for processing large amounts of data.

Apache's Hadoop Distributed File System is emerging as a superior s/w component for cloud computing.

However utilizing HDFS & MapReduce are not sufficient due to the fact that they do not provide adequate security mechanisms to protect sensitive data.

Security Issues:

By moving computing & storage needs to the cloud users can avoid high cost of storage & computing infrastructure and achieve availability & reliability at a relatively low cost.

However outsourcing storage & computing to a public cloud infrastructure introduces biggest challenges of data privacy & access privacy.

There are two important challenges in secure outsourcing, first the stored data need to be protected against unauthorized access. Second both data & access to the data must be protected from cloud storage providers.

In these scenarios depending on password & other access control mechanisms is insufficient & Cryptographic Encryption mechanisms are employed. In order to support both the challenges data should be encrypted first by the users before it is outsourced to a remote cloud storage service & data access privacy should be protected such that cloud service providers has no ability to decrypt the data & when the user wants to secure some parts of the whole data the cloud data storage systems must provide the accessibility without knowing what portion of the encrypted data is returned to the user is about.

In summary, a cloud storage service should meet the following three security and privacy requirements:

(a) **General data security:** The data should be securely stored in database hosted by the cloud storage service such that any unauthorized users cannot access it;

(b) **Database security:** A user is allowed to retrieve some data by keyword search techniques, but the user cannot get more content than the searching result;

(c) **User query privacy:** The user's query preference may be sensitive, and the cloud storage provider and its database server should not learn any useful information about which search keyword was submitted by the user and which data has been obtained by the user.

In addition to meeting the security and privacy requirements outlined above, the cloud storage service should continue to honor the generally accepted service level agreements (SLAs). That is, the cloud storage service should provide high computation and communication efficiency and support query-based access to allow users to selectively and privately retrieve any desired segment of the whole data on demand.

Cryptographic storage techniques are widely recognized as an approach that holds the potential to meet the above requirements. The main advantage of cryptographic storage services is that its security properties are derived from cryptography, as opposed to legal mechanisms, physical security or access control, and can be proved in a formal manner. A simple solution for secure cloud storage is to encrypt the whole data and then store it in a database. To query any part of the data, one must download the whole encrypted data for decryption. Its computation and communication complexity is high, and it fails to meet the database security and user query privacy requirements [1].

Searchable encryption schemes are designed to efficiently solve security problems for remote cryptographic storage while enabling search for the expected contents corresponding to an encrypted keyword securely.

Searchable encryption techniques are commonly used to efficiently meet the above requirements. There are several types of searchable encryption schemes in the literature, each of which is appropriate to a particular application scenario.

Symmetric searchable encryption (SSE) scheme introduced in [2] is suitable for the setting where a party searching over the data is also the one who generates it. Such scenario is referred to as single writer and single reader (SW/SR) [4].

Asymmetric searchable encryption (ASE) is designed for the scenario where a party searching over the data can be different from the party who generates it [3]. Such scenario is referred to as many writers and single reader (MW/SR) [4]. Since writers and readers can be different, ASE schemes are more suitable for the setting with a larger number of users.

Both SSE and ASE protocols do not completely solve the problem that one can privately retrieve segments of encrypted data from remote databases. Since the database server can learn by passive logging with statistical inference which encrypted keyword matches the submitted search keyword and which encrypted document is retrieved.

Conclusion:

We are conducting research on secure cloud computing. Due to the extensive complexity of the cloud we contend that it will be difficult to provide a holistic solution in securing the cloud at present. Therefore our goal is to make increment enhancements to secure the cloud that will ultimately result in a secure cloud. In particular we are developing a secure cloud consisting of h/w, s/w and data. Our cloud system will be efficient in 1) supporting efficient storage of encrypted sensitive data, 2) store, manage and query massive amounts of data, 3) support fine grained access control and support strong authentication. Building trust applications from un trusted components will be a major aspect with respect to cloud security.

References:

[1] C. Wang, K. Ren, Sh. Ch. Yu, et al. Achieving usable and privacy-assured similarity search over outsourced cloud data. INFOCOM, 2012.

[2] Y. Z. Tang, T. Wang, L. Liu, et al..Privacy-preerving indexing for eHealth information network, Proceedings of 20th ACM CIKM, 2011.

[3] D. X. Song, D. Wagner, A. Perrig. practical techniques for searches on encrypted data. Proceedings of the IEEE

Symposium on Security and Privacy, 2000, pp. 44-55.

[4] Joshi, J.B.D., Gail-JoonAhn. Security and Privacy Challenges in Cloud Computing Environments.IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.

[5] FarzadSabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[6] M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.

[7] Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.

[8] W. Stallings. Cryptography and Network Security: Principles and Practice. (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[9] S. Kamara, K. Lauter. Cryptographic cloud storage. The 14th international conference on Financial cryptograpy and data security, 2010, Springer-Verlag, pp. 136-149.

[10] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[11]. Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/hipods/library.html, October 2007, pp. 4-4

[12] G. Frankova, Service Level Agreements: Web Services and Security, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, vol. 4607.